Information Attack:
Information Warfare In 2025

A Research Paper
Presented To

Air Force ***2025***

by

Professor George J. Stein
Air War College

August 1996

Disclaimer

2025 is a study designed to comply with a directive from the chief of staff of the Air Force to examine the concepts, capabilities, and technologies the United States will require to remain the dominant air and space force in the future. Presented on 17 June 1996, this report was produced in the Department of Defense school environment of academic freedom and in the interest of advancing concepts related to national defense. The views expressed in this report are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States government.

This report contains fictional representations of future situations/scenarios. Any similarities to real people or events, other than those specifically cited, are unintentional and are for purposes of illustration only.

This publication has been reviewed by security and policy review authorities, is unclassified, and is cleared for public release.

Contents

Executive Summary

Information Attack is defined by the USAF as either "directly corrupting adversary information without changing visibly the physical entity in which it resides." or "activities taken to manipulate or destroy an adversary's information without visibly changing the physical entity within which it resides."

This essay argues that the proper understanding and future development of information attack, based on USAF information warfare competencies and systems, is the key to information dominance. It is likewise argued that a central obstacle to a future information warfare capability is that the words and definitions currently used among the Joint Staff and the armed forces to guide future development in IW are unclear, confused, and often contradictory as they fail to distinguish IW from Command and Control Warfare (C2W) and fail completely to incorporate USAF views on information attack.

The future potential in information warfare to substitute precise and discriminate credible information— whether by the methods of C2W (deception, PSYOP, or other means) or information attack— to a precise and discriminate target decision maker is the essence of decisive maneuver as it may position the adversary in space and time, by his own decision, in a fatally disadvantageous strategic situation. Information attack is not so much perception management as orientation management. Information is both the target and the weapon: the weapon effect is predictable error.

In future operating environments marked by ambiguity, speed, and precision effect, it will be the relative or differential advantage in information, information processing, and communication and information security that will provide the narrow margin for victory. Future USAF mastery of information attack, through air and space power unconstrained by artificial notions of battlefield-only command and control warfare, will provide the capability for asymmetric strategic response based on decisive and differential information advantage.

Chapter 1

Introduction

The strategic problems faced by the United States in the five 2025 alternate futures and the strategic problem faced in the intermediate world of 2015 identified in the *Air Force 2025 Study* are identical. The strategic problem faced by the armed forces in any of these futures is the same. "The true aim," as B. H. Liddell Hart observed, "is not so much to seek battle as to seek a strategic situation so advantageous so that if it does not of itself produce the decision, its continuation by a battle is sure to achieve this." [1] The question is whether information warfare and information attack can create this strategic situation in 2025 or even as early as 2015.

For the purposes of this essay, and for reasons which will hopefully become clear as the argument is developed, information warfare is defined as "actions taken to achieve relatively greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure in order to deny, exploit, influence, corrupt, or destroy those adversary information-based activities thorough command and control warfare and information attack."

Information warfare is normally understood, following the *Joint Publication (Pub) 3-13, Joint Doctrine for Command and Control Warfare (C^2W)* definition, as "actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while defending our own information and information systems."[2]

Information warfare is currently defined by the USAF as "Any action within the information environment taken to deny, exploit, corrupt, or destroy an adversary's information, information systems, and information operations, while protecting friendly forces against similar actions."[3] For the USAF, then,

bombing an enemy telephone exchange with iron bombs or corrupting the adversary's telephone switching system through electronic warfare or a computer attack are all, equally, information warfare. It is the targets, not the method of combat, which define information warfare for the USAF.

Command and control warfare is defined, following *Joint Pub 3-13, "Joint Doctrine for Command and Control Warfare (C^2W),"* as "a war fighting application of IW in military operations {that} employs various techniques and technologies to attack or protect a specific target set - command and control."[4]

Joint Pub 3-13 further defines C^2W as the "integrated use of psychological operations, military deception, operations security, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C^2 capabilities while protecting friendly C^2 capabilities against such actions."[5]

For the USAF, C^2W is simply "the effort to disrupt and destroy an adversary's command and control."[6]

Information attack is defined by the USAF as either "directly corrupting adversary information without changing visibly the physical entity in which it resides."[7] or "activities taken to manipulate or destroy an adversary's information without visibly changing the physical entity within which it resides."[8]

Thesis

The thesis of this essay is that the proper understanding and future development of information attack within the context of the USAF core competency of Information Dominance is the key to information warfare in the future.[9] It is likewise argued that a central obstacle to a future information warfare capability is that the words and definitions currently used among the Joint Staff and the armed forces to guide future development in IW are unclear, confused, and often contradictory.

The USAF strategy for information warfare should be well advanced by 2015 and fulfilled by 2025 through its incorporation within the central USAF mission of the employment of air and space power. Air and space power will, as today, be conceived as global awareness, global reach, and global power. Information warfare, especially information attack, will be employed as an expression of global power made possible through global awareness and global reach. It will provide an essential component of the global presence through which national security objectives will be met and will meet the national military strategy

of deterrence, promoting stability, thwarting aggression, and containing conflict, and, ultimately, projecting power to fight and win.

The key strategic issue will remain "not so much to seek battle as to seek a strategic situation so advantageous so that if it does not of itself produce the decision, its continuation by a battle is sure to achieve this." Information warfare, especially information attack, will provide the differential advantage, especially through air and space power, to permit the United States to develop and employ asymmetric modes of operation at what are called currently the strategic, operational, and tactical levels of conflict. Asymmetric and differential strategy is the key to breaking the platform-to-platform thinking (tank-counter-tank, ship-antiship, etc.) that continues to dominate long-range strategic thinking inherited from the successful experience in industrial-age warfare. Information warfare is the key to asymmetric and differential strategy and, in the context of this essay, information attack as new forms of air and space power are the key to information warfare.

The Future Environment

The development of asymmetric and differential strategy is required by the change in the range of potential military operations facing the armed forces in the emerging international security environment and the constraints consequent of both downsizing and the ever-increasing costs of traditional platforms.[10] While there may not be a settled consensus on the precise outlines of the emerging security environment, virtually all studies recognize that an unusually high plurality of diverse and untraditional tasks will challenge America's armed forces. The contemporary security environment is viewed as a generic regional contingency (or two nearly simultaneous major regional contingencies such as North Korea and Iraq), a generic niche competitor such as transnational criminal syndicates or ideological terrorists, or a generic, and yet to emerge, peer competitor.[11] The security environment can be seen as the *Air Force 2025 Study's* five alternate futures "Gulliver's Travails," "Zaibatsu," "Digital Cacophony," "King Khan," and "Halfs and Half-Naughts" and the 2015 "Crossroads" intermediate future. The security environment can be described more expansively as a range of high or low end global competitors, high or low end regional competitors,[12] counter-insurgency,

peace or humanitarian operations, dangerous industrial activities, weapons of mass destruction proliferation, collapsing or disintegrating states, and nonstate terrorism.[13]

The point is not that the armed forces will have to address all these challenges but that, despite downsizing and increasing platform costs, the military could be required to address any of these challenges. Absent the sudden emergence of a genuine competitor seen by the United States as having the capability to threaten American vital national security interests on a global basis, the armed forces, quite simply, must be able to do more with less or, perhaps as argued in this essay, must be able to do more by doing it differently. Information warfare through air and space power may provide the capability for asymmetric response through the differential advantage of information attack in most future security challenges.[14]

In the emerging information age and the operational environments postulated in almost all the alternate futures surveyed, military operations will reflect the characteristics of the larger societies.[15] As most armed forces and many military operations become increasingly dependent on information,[16] military winners will, like economic winners in the information-based economies, need to have that core competency identified by the USAF as information dominance whereby the United States has "greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure" than any adversary has about the United States.[17] Information independence and information security, whereby American military power projection and even mobilization are not vulnerably dependent on the global information infrastructure, will likewise emerge as central national security issues.[18] Any discussion of information warfare, including information attack, must be understood to include equal or greater attention to defense.

The goal of information dominance, note well, is greater understanding, not total understanding. As in the emerging information economies — sometimes called winner take all economies — "victory" is often based on a very small margin or differential of talent, information, performance, or luck. It is the relative performance in those markets or activities in which having or being second-best is inadequate, even at lower cost, which brings disproportionate rewards.[19] The Olympic gold medalist who is only two seconds faster than her silver second gets the running shoe endorsement contract. The F-16 pilot who locks on only two seconds faster gets the kill. By 2025, or surely by 2050, only will be nanoseconds.

Another novel characteristic of differential performance in information-based activities is the ability to duplicate and distribute the output of the differential activity more widely, more rapidly and at relatively lower cost. Once a recording company suspects it has a platinum compact disc among its releases, millions of additional copies can be quickly manufactured, distributed, advertised, and sold planetwide.[20] Once one component of the distributed reconnaissance and surveillance satellite system locks on the target, the coordinates are duplicated and distributed by an information and communications meta-system to its customers planetwide.

The ability to conduct information-age warfare through the relatively better use of information-in-war and the ability to duplicate and distribute information warfare itself through information attack may provide the relative or differential "strategic situation so advantageous" of which Liddell Hart spoke that Sun Tzu's pinnacle of excellence could be achieved wherein the enemy is subdued by asymmetric response without battle.

Information warfare, information-age warfare, information-in-war, information, and information attack are intimately related, but they are not identical. Clarification is needed and some consensus must be reached without, however, prematurely establishing authoritative doctrine that could prevent the creative developments required to realize the future potential of information warfare. The Joint Staff was correct when it noted in *Joint Pub 3-13* that the use of the term warfare in information warfare "should not be construed as limiting IW to a military conflict, declared or otherwise."[21]

Notes

[1] B. H. Liddell Hart, *Strategy* (London: Faber and Faber Ltd., 1967), 325.
[2] Joint Pub 3-13, "Joint Doctrine for Command and Control Warfare (C^2W) (draft)," 1995 I-4.
[3] *USAF, Air Force Doctrine Document-5 (1st draft), (November 1995), 20.*
[4] Joint Pub 3-13 v.
[5] Ibid., I-4
[6] USAF, Air Force Doctrine Document-5, 18.
[7] USAF, Cornerstones of Information Warfare,.6.
[8] USAF, Air Force Doctrine Document-5, 19.
[9] Gen Ronald R. Fogleman, USAF, Chief of Staff and Sheila E. Widnall, Secretary of the Air Force, Air Force Executive Guidance, (1996) 4.
[10] Theresa Hitches, "Lawmakers Call '97 Clinton Plan Unrealistic," *Defense News*, 11-17 March 1996, 14.

[11] Jeffery R. Barnett, *Future War: An Assessment of Aerospace Campaigns in 2010* (Maxwell AFB, Ala. Air University Press, 1996).

[12] Jason Glashow, "Regional Powers May Gain Clout," *Defense News*, 11–17 March 1996, 36.

[13] *Board of Directors, USAF Long Range Planning, "Future Operating Environments," Briefing Slides 29 February 1996,: R33.*

[14] Joseph S. Nye and William A. Owens, "America's Information Edge," *Foreign Affairs*, March/April 1996, 20-54.

[15] Pat Cooper, "Information Whizzes To Advise DoD on Future Wars," *Defense News*, 26–3 February March, 1996, 14.

[16] Len Zuga, "EW Competition to Surge," *Defense News*, 19–25 February 1996, 20.

[17] USAF, *Air Force Doctrine Document-1 " Air Force Basic Doctrine*," (draft) 15 August 1995, 10

[18] Pat Cooper, "IW Study May Guide U.S. Policy," *Defense News*, 25–31 March, 1996, 39.

[19] Steven Pearlstein, "The Winners are Taking All," *Washington Post National Weekly Edition* 13 11–17 December 1995, 6-10.

[20] Gary Hamel and C. K. Prahalad, *Competing for the Future*, (MA: Harvard Business School Press, 1994).

[21] Joint Pub 3-13, .I-4.

Chapter 2

New Ideas - New Words

The basic problem with understanding information warfare today is that there is no clear sense of just *what* is being discussed. The futurists Alvin and Heidi Toffler have argued in their recent book *War and Anti-War* that the United States armed forces need to develop a systematic, capstone concept of military "knowledge strategy" which would include clear doctrine and policy for how the armed forces will acquire, process, distribute, project, and protect knowledge and information to serve national strategy.[1] The Tofflers and others have argued that the concept of information warfare includes those information-based operations which attempt to influence the "emotions, motives, objective reasoning, and ultimately the behavior" of others.[2] The strategists John Arquilla and David Ronfeldt, on the other hand, have argued in their important essay "Cyberwar is Coming!" that "netwar" and "cyberwar" are the key concepts for understanding information war.[3]

Originally emerging in the science fiction community as, for example, in the very thought-provoking future war suggested in Bruce Sterling's *Islands in the Net,*[4] the concepts of netwar and cyberwar provide one thoughtful starting point for exploring the military and civil/military issues of information war. Netwar, according to Arquilla and Ronfeldt, is a "societal-level ideational conflict waged in part through internetted modes of communication." That is, they suggest that what is today seen as *strategic- level,* traditional, state-to-state conflict through the use of a nation's electronic intelligence and communications assets is the essence of netwar. Unlike traditional propaganda that seeks to provide information (whether true or false) which the adversary must understand, netwar or *strategic* level information war attacks another society's epistemology and decision-making process. Netwar attacks how the adversary knows, not just what the adversary knows.

Cyberwar is seen as the *operational* level of information warfare whereby the armed forces use netwar principles, techniques, and technologies to attack the epistemology and decision-making process of the enemy armed forces— especially its commanders. Most current discussion of information war in the armed forces seems to focus almost exclusively on the tools and techniques of cyberwar rather than strategic-level netwar. At the operational level of war, a national information war or netwar strategy would be translated by the armed forces into cyberwar or command and control warfare, often referred to in military shorthand as C^2W. Cyberwar, in the hands of the local military commander, attacks the mind of the enemy commander through various tools, many of which are from the universe of electronic warfare, to produce bad decisions and prevent, delay, or deny information for good or militarily effective decisions.

For the purposes of this essay, information warfare is seen as analogous to netwar and, as noted above, from within the USAF view, as "actions taken to achieve relatively greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure in order to deny, exploit, influence, corrupt, or destroy these adversary information-based activities thorough command and control warfare and information attack."

Command and control warfare would be understood by the armed forces as analogous to cyberwar. Information attack, recall, is "*directly corrupting adversary information without changing visibly the physical entity in which it resides*" and is the key to both netwar and cyberwar.

Within the general and authoritative military context, however, there is little agreement on definitions or the scope of the debate. Words have meaning as, at least, the components of military doctrine and, as such, affect how each service will "organize, train, and equip" its forces to support national security policies. Much of this essay may seem to be mere semantic nit-picking, but the "right" words and definitions are vital because of the authoritative nature of doctrine. The services fight over words. [5] Whether each service will be able to make informed decisions on the future evolution of the armed forces depends on their having a coherent understanding of the promise and perils of information warfare and, especially, information attack.

As the service most likely to be able to develop its current information warfare assets embedded in global awareness and reach, and its information attack potential in global power, the USAF has a special and historic responsibility to lead clear thinking and doctrinal development for the new forms of strategic operations permitted by information warfare and information attack.

[1] Alvin and Heidi Toffler, *War and Antiwar: Survival at the Dawn of the 21st Century* (Boston: Little, Brown & Co., 1993),141.

[2] Joint Chiefs of Staff Memorandum of Policy 30, *Command and Control Warfare* (March 1993), A-4.

[3] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy* 12, no.2 (April–June, 1993), 141-165.

[4] Bruce Sterling, *Islands in the Net* (NY: Ace, 1988).

[5] The continuous argument over the "authority" of the Joint Force Air Component Commander (JFACC) to "control" ground-support missions is illustrative. To the outsider the debate seems "theological." To troops on the ground, it's a question of life or death.

Chapter 3

Confused Visions

A key problem within military discussions of information warfare is that the Department of Defense, the Joint Staff, and each individual service recognize that if IW is, indeed, a new form of warfare or represents a potential for a true "revolution in military affairs," then there are important implications for the traditional roles and missions of each individual service. If, for example, "to be seen is to be killed" and hostile unmanned aerial vehicles (UAV) provide battlefield overview for smart artillery shells, armored units whose own air and space forces have not yet "blinded" the enemy will be sitting ducks. This, likewise, has implications for future access to increasingly scarce defense appropriations. If, for example, Congress becomes convinced that investing in swarms of cheap-tank-locating UAV for US Army helicopters to use to kill enemy tanks is a better idea, then this raises the obvious question "Why are we still buying tanks?" Indeed, Congress might ask whether the Joint Strike Fighter (JSF) is the better investment for plinking tanks in open terrain than an uninhabited combat air vehicle (UCAV). The military is, understandably, institutionally conservative and, as in the early discussions of airpower or current discussions of space power, more likely to attempt to fit the new into the already known.[1] Even the USAF has a legacy of platform-focused thinking.[2]

On the other hand, information warfare is the hot topic of the age and everyone wants to the part of the "Third Wave," the armed forces being no exception. Unfortunately, far too much discussion in the armed forces of IW confuses the traditional importance of information-in-warfare with information warfare or information attack itself. All those papers and briefings that begin "Information has always been central to warfare. . ." and then go on to explain that "our new computer system will get information to the warfighter" so he can "achieve information dominance on the battlefield" and thus demonstrate our service's mastery of

IW, confuse information-in-war with information warfare. Whether we are digitizing the cockpit or digitizing the battlefield, this is not IW.[3] Information-in-war is absolutely vital and will be an increasingly important issue as the use of information is central to modern warfare and, more importantly, may be the *sine qua non* or necessary-but-not-sufficient condition for the conduct of any future traditional warfare and certainly any future information warfare. A review of the current debate within the armed forces will illustrate the problem. Ultimately, a particular USAF idea will point to the solution.

The Joint Staff

While the current draft definition is unclassified, the official definition of *information warfare* remains classified top secret. The public, nonclassified and formal military discussion of information warfare began with the Joint Chiefs of Staff *Memorandum of Policy (MOP) - 30* (1993), "Command and Control Warfare." This document set the initial terms of debate and, consequently, most formal debate since. Most importantly, "Command and Control Warfare" or C^2W was defined as "the military strategy that implements Information Warfare on the battlefield" and its objective was to "decapitate the enemy's command structure from its body of forces."[4] The legacy of Desert Storm's airpower and electronic warfare against Iraq was seen as the essence of information warfare.[5] What is really being discussed in the desert war context is, in fact, the new and creative use of information-in-war noted by Soviet and other observers.[6] Note also that the discussion of IW starts as a battlefield topic with the result that much of the continuing debate places IW in the combat support role rather than as a new form of combat proper.

More recently, the Joint Staff has expanded the idea of information warfare in *Joint Pub 3-13* (1995), "Joint Doctrine for Command and Control Warfare." Information warfare is defined, as noted above, as actions "taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending friendly information systems."[7] Here, a central and vital issue is noted. While the armed forces may attempt to gain superiority by affecting adversary information and information systems, they can defend only friendly systems. That is, the Joint Staff seems to assert that the armed forces have no military mission or authority, currently, to defend friendly information. The armed forces, it appears to be claimed, can protect military information systems

only; they cannot use military assets to defend the nonmilitary information systems of the United States from adversary attempts to gain military advantage. The political debates about the restrictions placed on conveying pornography on the Internet contained in the Communications Decency Act accompanying the recently enacted Telecommunications Act are a mere skirmish compared to the civil libertarian firestorm that would result if the military claimed a role in nongovernmental information or information systems protection.[8] On the other hand, the mission of the armed forces is to defend the United States, and if hostile information attack threatens the national security, it is difficult to see why the skills and experience that the armed forces are developing to protect military systems should not be loaned to an interagency Information Security Task Force.

The Joint Staff's *Joint Pub 3-13* then modifies the earlier definition on command and control warfare (C^2W) first used in *MOP-30* in an important but ultimately inadequate way. C^2W is now seen as "a {not *the*} war fighting application of IW in military operations {not just on the *battlefield*} and employs various techniques and technologies to attack or protect command and control {not just *decapitate*}". *Joint Pub 3-13* goes on to define C^2W as the "integrated use of psychological operations, military deception, operations security, electronic warfare, and physical destruction, mutually supported by intelligence." That is, the integrated use of perfectly traditional information-in-war tools and techniques.

New Thinking?

The Joint Staff, whose views on doctrine are assumed to be directive for the individual services and whose definitions thereby amplify the importance of words, is currently developing a series of ideas for war fighting in the near-future: *Joint Vision 2010 - America's Military: Shaping the Future*. While not focused primarily on information warfare, *Joint Vision 2010's* ideas are of direct relevance to the future evolution and role of IW. *Joint Vision 2010* begins with a projection of current technological trends assumed to shape the future war fighting environment. These include: (1) the increasing precision of weapons and their means of delivery, (2) the increasing menu of weapons' effects from traditional lethality to nonlethal technologies, (3) increased stealth for both offensive platforms and invisibility of friendly forces, and (4) improvements in

information systems integration, from sensors to shooters, which may permit a "dominant battlespace awareness" to include the ability to "see, prioritize, assign, and assess."[9]

These four trends, which are assumed to provide a magnitude improvement in lethality, will require information supremacy. Information supremacy is defined here as the "capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[10] This is, of course, both a worthy goal and a perfect definition of information-in-war. Information supremacy, according to *Joint Vision 2010*, will require both offensive and defensive information warfare. Offensive IW will degrade or exploit an adversary's collection and use of information and will be conducted by traditional and "nontraditional" means such as "electronic intrusion" into an information and control network to "convince, confuse, or deceive enemy military decision makers."[11] Defensive IW will protect dominant battlespace awareness and provide improved command and control of friendly forces and will be conducted by traditional means such as physical security and encryption and untraditional means such as antivirus protection and secure data transmission.

Joint Vision 2010, then, continues the pattern of seeing information warfare as an advanced version of command and control warfare (C^2W), new techniques of traditional electronic warfare (EW), and a sense that computer viruses, as a form of EW, might be important. Information supremacy is still defined, operationally, as information-in-war rather than information warfare as a potentially new form of warfare for the future. This most current Joint Staff thinking appears to have forgotten its earlier idea in *Joint Pub 3-13* that the use of the term warfare in information warfare "should not be construed as limiting IW to a military conflict, declared or otherwise."

Based on the technologies of this information supremacy providing dominant battlespace awareness, *Joint Vision 2010* proposes that new concepts of operation will need to be developed. These new operational concepts (how the joint force commander will fight the fight with land, sea, air, and space forces assigned) are (1) dominant maneuver, (2) precision engagement, (3) full-dimension protection, and (4) focused logistics. These four new operational concepts will provide "Full Spectrum Dominance" to achieve massed effects in warfare from dispersed forces across the spectrum of military actions from peacetime engagement through deterrence and conflict prevention to fight and win warfare.

The key problem with Full Spectrum Dominance is not only that its notion of information warfare is still too focused on information-in-warfare but that the application of massed effects in warfare from dispersed forces still appears to assume that massing forces is the strategic problem. The Joint Staff appears to assume, naturally enough, that land, sea, air, and space forces are the only, or certainly major, means for the joint force commander to accomplish the mission. That militarily-relevant, strategic, operational, or tactical effects might be produced by information attack without combining the various joint forces in theater may be the key difference between information-in-warfare and information warfare. A brief survey of the four new operational concepts will illustrate the problem.

Dominant Maneuver

Dominant maneuver is an operational concept that grows from the experience of the Gulf War and the evolution of US Army thinking from "Air-Land Battle" to "Force XXI Operations."[12] In essence, instead of warfare being conducted as a series or sequence of battles leading ultimately to the enemy collapse, dominant maneuver proposes to bring together widely dispersed joint forces to attack the enemy throughout the height, breadth, and depth of the battlespace by attacking all levels of the enemy's centers of gravity simultaneously.[13] Clearly, the increasing precision of weapons and their means of delivery, the increasing menu of weapons' effects from traditional lethality to nonlethal technologies, the increased stealth for both offensive platforms and invisibility of friendly forces, and the improvements in information systems integration are the technologies that permit dominant maneuver. *Joint Vision 2010* recognizes that these new weapons will "allow us to conduct attacks concurrently that formerly required massed assets in a sequential methodology."[14] And, while these new weapons and technologies may permit us to "accomplish the effects of mass — the necessary concentration of combat power at the decisive time and place — without physically massing forces," dominant maneuver still appears to seek to "attain with decisive speed and tempo a *physical* presence that compels an adversary to either react from a position of disadvantage or quit." (emphasis added). *Joint Vision 2010* is confused. Do mass effects require physical presence by joint forces assembled from widely dispersed locations or not? And why does *Joint Vision 2010* assume that mass

effects are superior to differential effects? Information warfare, advanced C^2W, and information attack may not need to share this assumption.

Precision Engagement, Full-Dimension Protection and Focused Logistics

Precision engagement and full-dimension protection make the same assumption. Precision engagement depends on a system of systems[15] that permits our forces to locate the target, provide responsive command and control, have the desired effect, assess the effect, and reengage if required. That is, we can shape the battlespace and conduct a dominant maneuver. Full-dimension protection, built on information supremacy (actually, supremacy of information-in-war), will provide multidimensional awareness and assessment, as well as identification of all forces within the battlespace. Defensive information warfare will be required to protect our information systems and processes.

Focused logistics, the final new operational concept, again illustrates the thinking that the ability to project power with the most capable forces is the central problem. The ability to fuse information, logistics, and transportation technologies; provide rapid crisis response; track and shift assets even while enroute; and deliver the logistics and sustainment to the level of operations" assumes that getting stuff there for the forces is the essence of projecting power. Yes, in many cases, especially against traditional adversary's armed forces or other military operations like peace enforcement and humanitarian relief, this may be true.

Dominant maneuver, precision engagement, and full-dimension protection are clearly operational concepts that will permit the US armed forces to attain full spectrum dominance in a traditional campaign against a traditional adversary. There will be undoubtedly Saddam-revenant adversaries even in 2025. Creative USAF thinking about information warfare, however, requires that a series of unusual questions be asked: What is the future battlespace. What are forces in future conflicts? What is "there" in a future battlespace? What if the adversary is not employing forces?

Joint Vision 2010 introduces a generally thoughtful and potentially useful set of ideas for the evolution of operational concepts for US joint forces to employ in traditional military operations across a large spectrum of conflict. It correctly recognizes information-in-warfare as one of the most important and critical aspects of near-future (*circa* 2010) military operations. Information superiority is, in fact, the necessary

condition for future joint warfare and, as such, the Joint Staff is correct in calling for far greater attention to the promise and peril of the new technologies for the collection, processing, and secure dissemination of information-in-war. *Joint Vision 2010* is much less successful in addressing the implication for the US armed forces, and especially the USAF, if the potential for information warfare were to be something beyond a technology-based, more sophisticated version of command and control warfare.

It is, of course, the individual armed services that are tasked to organize, train and equip for the future. How are the individual armed services thinking about information warfare on the road to 2025?

The US Army

For the US Army, "information operations" replaces information warfare as the capstone concept. Information operations are continuous military operations within the military information environment that enable, enhance, and protect the commander's decision cycle and mission execution to achieve an information advantage across the full range of military operations.[16]

Information operations include "interacting with the global information environment and, as required, exploiting or degrading an adversary's information and decision systems." That is, the Army recognizes that information affects operations far beyond the traditional battlefield and, thus, information operations is seen as the proper "word" to include both information warfare and command and control warfare. This is a potentially important evolution in Army thinking but, currently, it results in a limited view of information warfare. information operations may, in fact, be a better word than information warfare, and could be adopted by the Joint Staff and the other services, but only if the concept is expanded to mean more than "military operations within the military information environment."

Information warfare, for the US Army, are actions taken to preserve the integrity of one's own information system from exploitation, corruption, or destruction while at the same time exploiting, corrupting, or destroying an adversary's information system and in the process achieving an information advantage in the application of force.[17] That is, information warfare remains in the universe of traditional platform-versus-platform thinking like "only armor can confront armor" with the information system as the new platform.

Information warfare thus has been constrained to the universe of the combat support elements where techno-wizards will provide advantage for Willie and Joe to apply force with real weapons like tanks and artillery.

The US Army appears to confuse information-in-war with information warfare. The Army's goal to "assimilate thousands of bits of information to visualize the battlefield, assess the situation, and direct military action appropriate to the situation" is the use of information-in-war for traditional battle. The Army's "Information Age" *Force XXI* will "know the precise location of their own forces, while denying that kind of information to their foes" because, for the Army, information is "an essential dynamic enabling dominant military power at the strategic, operational, and tactical levels." This will be achieved by "using and protecting information infrastructures" while influencing or denying a potential adversary's use of these infrastructures.[18]

By constraining its doctrinal thinking to the infrastructure aspects of information and adopting uncritically the Joint Staff definition of command and control warfare (C^2W), the US Army may have let its traditional, and proper, land-warfare focus prematurely narrow its vision to the battlespace of armor, artillery, and infantry divisions. While it is undoubtedly important that the Army study and apply its notion of information warfare to command and control warfare, it is also undoubtedly obvious that the Army must develop its concept of information operations beyond "the military information environment." information operations, if conceived synergistically with the USAF concept of information attack, are much more than "integrated support to battle command" in traditional military operations.[19]

The US Navy

The US Navy essentially shares the same view of information warfare as does the Air Force but, like the US Army, views information operations as a means through which to conduct traditional battle. Like the Air Force, the Navy views command and control warfare (C^2W) as distinct and subordinate to information warfare proper. Like the Army, the Navy appears to view IW primarily as a means to prepare for battle. The former chief of naval operations, Adm J. M. Boorda, observed recently that because of the Navy's traditional forward deployment, "Information Warfare will give us the ability to slow and influence the enemy's decision making cycle, to prepare the battlespace before the start of hostilities, and to dictate the

battle on our terms."[20] While naval doctrine for IW is in at least as much flux as that of the other services, current doctrine straddles the big view of IW and the little view of IW as C^2W. Operations Naval Instruction (*OPNAVIST)* 3430.26 defines IW as action taken in support of national security strategy to seize and maintain a decisive advantage by attacking an adversary's information *infrastructure* through exploitation, denial, and influence, while protecting friendly information *systems* [emphasis added].[21]

Platform-to-platform battle is again the model. Likewise, C^2W is the "action taken by the military commander to realize the practical effects of IW on the battlefield." As a service, the Navy may be expected to develop the tools and techniques of C^2W for power projection from the sea with the growing awareness of the potential for IW to project the effect of combat power far inland from the combat forces that are the source of that power.[22] The Navy recognizes that information warfare "encompasses political, economic, physical, and military infrastructures" and "expands the spectrum of warfare from competition to conflict."[23] There is an obvious potential for mutual synergy in developing asymmetric strategies between the Navy's sea and air assets and the US Air Force's air and space assets for both C^2W based information warfare and information attack.

The US Air Force

The US Air Force begins its reflections on information warfare from within its views on air and space power. For the USAF, air and space power are a means to an end, not the end itself. Like the Navy's "from the sea," air and space power are "done" in and from a "place" that is "more than a place": the air and space. Thus, air and space power include the projection of military force from air and space. The goal is air and space superiority as the necessary, but not sufficient, condition for the application or employment of all other military power. And, as air and space surround the globe, the USAF sees itself as having a global mission of air and space superiority, global mobility, and the precision employment of air and space assets. The same vision informs USAF thinking on information warfare.

For the USAF, currently, information is seen as analogous to air and space. Information is seen as a realm in which dominance will be contested and in which and from which military power can be employed. Like air and space power, information dominance is a necessary, but not sufficient, condition for the

application or employment of all other military power and, likewise, is a global mission. Mastering information warfare, then, will become a USAF core competency like air and space superiority. Unfortunately, USAF thinking currently suffers some of the same internal contradictions as does the IW thinking of the Army and Navy and, more importantly, that of the Joint Staff. The issue is, again, confusion among information-in-war, information, and information warfare.

The USAF recognizes correctly that information dominance is a broad concept and describes it, in Air Force Doctrine Document 1 (AFDD-1) "Air Force Basic Doctrine," in the war-fighting context as that condition in which the commanders have "greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure" than the enemy has about our side.[24] That is, information dominance provides a decisive degree of information-in-war that is essential for the successful application, enhancement, or employment of air and space power or, indeed, any other kind of military power. On the other hand, in Air Force Doctrine Document 5 (AFDD-5) "Information Warfare," information dominance is defined as that "degree of superiority in information functions that permit friendly forces to operate at a given time and place without prohibitive interference from opposing forces."[25] As will be discussed presently, information "functions" is a problematic limitation. While information dominance must become a core USAF competency by 2025, it is only one key step, potentially, toward full-information warfare competency. Like the US Army, USAF thinking on information warfare must not be constrained to "information functions."

Unlike *Joint Pub 3-13* (1995), "Joint Doctrine for Command and Control Warfare," USAF thinking on information warfare appears to see aerospace power as not constrained by political considerations from protecting the military forces against hostile enemy information actions. That is, for the USAF, IW is any action to "deny, exploit, corrupt, or destroy an adversary's information, information systems, and information operations" while protecting "friendly forces from similar actions."[26] While the Joint Staff, the Army, and Navy see part of IW as protecting our military *systems* and military information *infrastructure*, the USAF appears to envision part of IW as defending the armed forces against enemy information actions as well as defending the military information infrastructure. The USAF is right: waiting for an electronic Pearl Harbor and then beginning the slow buildup and deployment of Army land power to apply force is not the way to prepare the armed forces for the fight, or to deter fighting, in the information age.

Confusion

It must be admitted that current USAF thinking is confused in the area of information warfare and has not yet reached a coherence in the words that will define and guide doctrine. The USAF doctrine community, unfortunately dispersed among the Air Staff, the Air Force Doctrine Center at Langly AFB, the College of Doctrine, Research and Education at Air University, and the Air Command and Staff College and Air War College, must aim to harmonize its thinking. USAF long-range planning cannot incorporate the information warfare insights developed in research like *New World Vistas* or *Air Force 2025* without a coherent vocabulary. Words matter.Air Force Doctrine Document-1 (AFDD-1), Air Force Doctrine Document-5 (AFDD-5) and Cornerstones

Current (August 1995 draft) *Air Force Doctrine Document-1* (AFDD-1), "Air Force Basic Doctrine," and AFDD-5, "Information Warfare," postulate six roles for air and space power: control, strike, mobility, information, sustainment, and preparation. The information role is defined to include command, control, communications, and computers (C^4); intelligence, surveillance, reconnaissance, navigation and positioning; and the weather service. Clearly, information is seen like sustainment and preparation as combat support or combat service support to the war-fighting missions of strike, control, and mobility. According to *AFDD-1*, USAF core competencies, as in *Air Force Executive Guidance*, include air superiority, space superiority, global mobility, precision employment, and information dominance. As noted above, for AFDD-1, information dominance is that condition that gives greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure than the enemy has about our side. The core competency of information dominance, then, appears to be accomplished by the information role of air and space power.

In an attempt to provide the doctrinal foundation[27] for information warfare, the USAF chief of staff, Gen Ronald R. Fogleman, and the secretary of the Air Force, Sheila E. Widnall, issued *Cornerstones of Information Warfare* in 1995. *Cornerstones* proposes that the roles and missions of air and space power are not the six of *AFDD-1* but four: aerospace control, force application, force enhancement, and force support. Information warfare is not a separate role or mission but is incorporated as a component of aerospace power. In aerospace control, IW is counterinformation— actions dedicated to controlling the

information realm. Command and control warfare (C^2W) appears under the mission of "force application." Information operations, really any action involving information-in-war, is part of "force enhancement" while the role of information in "force support" is merely noted.[28]

Command and control warfare (C^2W) is central to all military discussions of IW and *Cornerstones* views C^2W part of the force application mission. Here the USAF has made its most distinctive and promising addition to IW thinking. *Cornerstones* modifies the model of C^2W proposed by the Joint Staff and adopted by the Army and Navy from the "integrated use of psychological operations, military deception, operations security, electronic warfare, and physical destruction, mutually supported by intelligence" to "psychological operations, military deception, security measures, electronic warfare, physical destruction, and information attack."[29]

Information attack, is defined in Cornerstones as "directly corrupting information without visibly changing the physical entity within which it resides."[30] The USAF is the first to recognize that IW is about information itself and not just information-in-war. IW is about ideas and epistemology, what is known and how it is known, and would be waged largely, but not entirely, through adversary information systems and infrastructures. The target of war is ultimately the human mind of the adversary decision makers and, in the information age, it is information itself that is, increasingly, the center of gravity of an adversary's military, political, social, and economic infrastructure. In reality, what Cornerstones is asserting is that information is not just a realm in which dominance will be contested, but rather, the realm is information. Information is both the target and the weapon.

The USAF has a better sense of command and control warfare than either *Joint Pub 3-13* or the Army documents. C^2W is seen by the USAF as a force application mission like interdiction or close air support and it would conduct C^2W through electronic warfare, psychological operations, military deception, physical attack, and security measures.[31] *Cornerstones* adds information attack to C^2W. As a force application mission, C^2W attack (especially information attack) can be used for strategic, operational, or tactical effect. Like strategic air and space power, C^2W is not just a battlefield support mission. C^2W for the USAF and the Navy is only a particular form of IW, and to restrain the Navy or the USAF to C^2W as the extent of its contribution to IW operations would be a foolish waste of sea, air and space power assets and capabilities.

The problem comes, however, with *Cornerstones'* foundation idea of information attack doctrine in the authoritative context of official USAF doctrine represented in AFDD-1.

The Problem

While AFDD-1 recognizes that information warfare could be used for neutralizing an adversary's will and capacity to make war, its view of information attack illustrates the same unimaginative platform-to-platform thinking as "only aircraft can contest aircraft for air superiority." That is, information attack is seen in AFDD-1 as the use of "computers and communications to directly attack the adversary's information *operations*."[32] At first glance, and given the Army understanding of information operations, this appears to move beyond attacking platforms. The problem is that an information operation is any activity that involves information *functions* and, most importantly, *Cornerstones* has defined information functions as the *technology-dependent* elements involved in the acquisition, transmission, storage, or transformation of information seen as data and instructions.[33]

Because AFDD-1, "Basic Doctrine" defines information as "the organized network of information functions that enhance employment of forces," and *Cornerstones* has defined information functions as the *technology-dependent* elements of the network, there is a danger that the very sophisticated idea of information attack may be seen as little different from the Army's notion of "using and protecting information infrastructures while influencing or denying a potential adversary's use" of these infrastructures. It is still a counterplatform model.

AFDD-5, "Information Warfare," on the other hand, has defined information attack as "activities taken to manipulate or destroy an adversary's information without visibly changing the physical entity within which it resides" and information functions as any activity involving the acquisition, transmission, or storage or information.[34] The key question is: Does the USAF recognize "any activity" beyond attacking (and defending) the technology-dependent information infrastructure as part of information attack?

Authoritative USAF thinking has not demonstrated how IW could be used for "neutralizing an adversary's will and capacity to make war" beyond a slightly more expansive notion of command and control warfare tied to tricky computer hacking to enhance the employment of forces. The USAF must rethink

AFDD-1 and AFDD-5 to realize the potential of information warfare implicit in a creative development of information attack. The USAF must also reject the idea that IW is only to enhance the employment of forces, and must break free of the mantra of jointness wherein air and space power are discussed only within the context of supporting the Joint Force Commander. Air and space power will permit information attack in 2025, and information attack may be the differential that permits asymmetric strategic operations by aerospace power alone in war and peace.

Notes

[1] Andrew F. Krepinevich, "The Pattern of Military Revolutions," *The National Interest*, no.37 (Fall 1995), 30–42.

[2] Carl H. Builder, *The Icarus Syndrome: The Role of Air Power Theory in the Evolution and Fate of the U.S. Air Force* (New Brunswick, N.J. Transaction Publishers, 1994).

[3] James M. Dublik and Gordon R. Sullivan, *Land Warfare in the 21st Century* (Carlisle Barracks, PA: US Army War College Strategic Studies Institute, 1993).

[4] Joint Chiefs of Staff Memorandum of Policy 30, 3.

[5] Edward Mann, "Desert Storm: The First Information War?," *Airpower Journal* 8, no. 4 (Winter, 1994) 4–14.

[6] Mary C. FitzGerald, *The Soviet Image of Future Wars: "Through the Prism of the Persian Gulf"* (Washington, D.C. The Hudson Institute, 1991) and V.K. Nair, *War in the Gulf: Lesson for the Third World* (New Delhi: Lancer International, 1991).

[7] Joint Pub 3-13, I-4.

[8] Daniel Brandt, "Infowar and Disinformation: From the Pentagon to the Net," *NameBase NewsLine*, No.11, October–December 1995, 11 available from: gopher://ursula.blythe.org/00/pub/NameBase/newsline.

[9] *Joint Vision 2010 - America's Military: Shaping the Future* (1995), 5.

[10] Ibid., 7.

[11] Ibid.

[12] United States Army Training and Doctrine Command, *Force XXI Operations: TRADOC Pamphlet 525–5* (August 1994).

[13] Ibid., 2–9.

[14] *Joint Vision 2010 - America's Military: Shaping the Future* (1995), 7.

[15] William A. Owens, "The Emerging System of Systems," *Military Review* 75 no. 3 (May–June, 1995), 15-19.

[16] United States Army Training and Doctrine Command, *TRADOC Pamphlet 525-69: Concept for Information Operations* (August 1995), 2.

[17] Ibid., 3.

[18] United States Army Training and Doctrine Command, *TRADOC Pamphlet 525-69*, 2.

[19] Ibid., 2.

[20] Air Land Sea Application Center, *Information Warfare / Information Operations Study* (December, 1995), 16.

[21] Ibid., 17.

[22] Navy Public Affairs Library, *Copernicus - Forward C4I for the 21st Century* (June 1995), 2.

[23] Ibid., 7.
[24] USAF, Air Force Doctrine Document 1, 10.
[25] USAF, Air Force Doctrine Document 5 , 19.
[26] USAF, Air Force Doctrine Document -1, B-3 quoting AFDD-31 (First Draft).
[27] USAF, Cornerstones of Information Warfare, 16.
[28] Ibid., 11.
[29] Ibid., 5.
[30] Ibid., 6.
[31] Norman B. Hutcherson, *Command and Control Warfare: Putting another Tool in the War-fighter's Data Base*, (Maxwell AFB, Ala.: Air University Press, 1994).
[32] USAF, Air Force Doctrine Document-1, 11.
[33] USAF, Cornerstones of Information Warfare, 2.
[34] USAF, Air Force Doctrine Document-5 19.

Chapter 4

Rethinking Information Warfare

The USAF strategy for information warfare will be developed by 2025 through its incorporation within the central USAF mission of the employment of air and space power. Air and space power will, as today, be conceived as global awareness, global reach, and global power.

The USAF has seen correctly that information is like air and space; it is a realm in which superiority will be contested and from which power can be projected or engagement conducted. Information, for the USAF, is likewise just as much part of the physical universe as the other realms in which it operates and, indeed, may be "the" realm. Thus, information warfare will be conducted according to the same principles as are air and space operations. If this axiom is correct, and there is no scientific reason to assume that information is not grounded ultimately in matter and energy, then the characteristics of information warfare are analogous or parallel, not merely metaphorical, to the contemporary and future characteristics of air and space power.[1] The contemporary and future characteristics of air and space power, and the key to its centrality to those differentials which argue that aerospace power is the instrument for an asymmetric strategy are, of course, global awareness, reach, and power. Global awareness provides, increasingly, exact and timely information. Global reach permits a range and responsiveness to engage, not just fight, throughout the global battlespace. Global power, increasingly marked by the ability to apply precise and discriminating effects of power, will permit an asymmetric response which leverages the differential information-in-war advantage provided by global awareness and the information-based planning and execution control provided by global reach.

Global Awareness

Global awareness, in the view of *New World Vistas: Air and Space power for the 21st Century*, is that the USAF can use "affordable means to derive appropriate information about one or more places of interest after a delay which is short enough to satisfy operational needs."[2] Global awareness requires the USAF to have the ability to detect and understand friendly and adversary activities in space, on the surface, and in the air. Global awareness in 2025 will require, additionally, detection and understanding in the info-realm or cyberspace. In the info-realm, global awareness must provide the information-in-war essential for information attack on the strategic, operational, or tactical centers of gravity of an adversary's military, political, social, and economic infrastructure.[3]

Various capabilities to provide global awareness to support traditional air and space power employment will, obviously, be vital in providing for the employment of information attack in the alternate and intermediate futures of the *2025 Study* and, indeed, any future security environment. There are also info-awareness-specific capabilities that will need to be developed.

The set of required capabilities for future global awareness include a new generation of sensors based on a distributed system of satellites, surface sensors, and standoff systems based possibly on Uninhabited Combat Air Vehicles (UCAV).[4] As it may be too much to expect even the new Joint Requirements Oversight Council to force the development of a common USAF /Army/Navy system and standards of database management and data communication, an implied requirement of continued USAF leadership of the global awareness system is a generic crosstalk capability with sister services and coalition partners.[5]

A specific set of USAF requirements for information attack, defined as directly corrupting information without visibly changing the physical entity within which it resides, can be identified within the general requirement of database management within global awareness. As in the classic North American Air Defense Command nuclear attack defensive system, the information must be detected and identified before there can be any talk of interception or destruction. Consequently, a reorientation in thinking about the traditional target sets for militarily-relevant intelligence gathering needs to occur as the information warfare battlespace is the information-dependent global system-of-systems on which most of the "strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure"

increasingly depend. That is, not only must the question "What and where are the data?" on which these infrastructures depend be answered, but, equally important, "What are the structures and patterns of human activity depending on these databases and communications infrastructures?" Information attack requires more than a knowledge of wires and, consequently, suggestions for an Information Corps of techno-wizards would only produce platform thinking as hackers fought hackers.[6]

Locating and corrupting a database that is of marginal relevance to an adversary's will and capacity to make war is a waste of scarce resources. It is the relevant information differential that is central to information attack as apparently benign activities or databases can hide potentially hostile cyber-strike capabilities. Thus, while global awareness for information attack appears to be about "everything," at the pragmatic level, artificial intelligence search-architectures for differentially-relevant "information" must be designed by the Air Force Intelligence Agency, the Air Force Institute of Technology, and other labs under the Air Force Material Command. The technologists, however, must be led by the strategists in the same way as planning the traditional air campaign requires a coherent knowledge of the adversary systems.[7] It is the patterns of human activity that are central.

As asymmetric response may be the best strategic choice in many cases, the relevant information target for global awareness attention may not be those data and communications systems that support directly the adversary's fielded military activities, (the Joint Staff's nominal target for information warfare and the adversary systems most likely to be best defended), but those other supporting data, infrastructure, and patterns of activity on which most contemporary and future military operations depend. While specific information attack activities will be discussed below in the section on global power, one example of the "other" data systems which might be subject to discriminate or precision asymmetric information attack are an adversary's Supervisory Control and Data Activity (SCADA) systems for the operation of the air traffic control or fuel pipeline network.[8] Clearly, then, the SCADA data bases and networks of potential adversaries must be detected, identified, and mapped.

At the most generic and nontechnical means level, global awareness for information attack will require monitoring commercial developments in information infrastructure architectures and capabilities, among whom these systems are employed, and how and by whom they are used. And, as it should be obvious that there is a defensive aspect of information warfare in that these capabilities will be used by an adversary

against the United States or an ally, careful monitoring will be required of developments in commercial-off-the-shelf (COTS) systems which could be used to attack industrial processes (for example anti-SCADA programs), financial and communications networks, and break-through systems that might provide differential advantage in information management and communications. Equally important, patterns of human activity or organizational change that suggest a developing potential for hostile information attack must become part of the normal business of global awareness. Identification of commercial industrial espionage in info-systems, even by an ally, should be presumed to indicate the intent to develop an information attack capability.

To support information attack in the near-future, whether for information warfare or C^2W, USAF global awareness systems will need to develop and incorporate specific database and database management and correlation acquisition to its collection, processing and analyzing of activities currently monitored for planning and execution control.[9] This set would include, logically, standard intelligence and surveillance architectures, command, control, and communications systems, especially systems designed to detect and defeat information attack, target and tracking, guidance, and navigation systems, especially space-based and other long-range communication capable systems, and attack assessment and reconstitution systems.[10] The intelligence challenge will be more demanding than when the United States faced only one strategic peer competitor.

To support future capabilities for information attack in the asymmetric engagements required in the *2025 Study*, current USAF global awareness and monitoring activities will need to be expanded to include the other database and database management information systems. These might include general computer systems such as the internet and the world wide web, power generation and distribution systems, industrial, financial and transportation systems, and, in general, any system which might be used by an adversary to launch an information attack, first on US armed forces, and ultimately, on other domestic information assets.[11] Such an expansive system of monitoring will be essential to protect these domestic assets on which US joint force power projection itself ultimately depends.

It is important to note that the reorientation of intelligence activities needed to support information attack (and defense) in both the near and 2025 future as a USAF global awareness mission is in complete conformity with current US law. The object of USAF global awareness is not the American domestic database and database management systems. Domestic counter intelligence and law enforcement agencies

will develop an ability to monitor adversary activities in the United States. On the other hand, USAF global awareness assets may be the main source of intelligence support for alerting law enforcement agencies charged with protecting domestic information-dependent activities from adversary information attack about hostile capabilities.[12]

Global Reach

Global reach is usually thought of as the ability of deploy aircraft from the Continental United States or out-of-theater bases into the area of interest in a rapid and timely fashion. The role of air refueling is likewise central to global reach. Whether delivering bombs, special forces troops, or humanitarian assistance, the speed, range, and lift of aircraft are usually seen as the key issues in delivering what is required. This differential ability to reach out with rapid, discriminate, and precise effect is central to the USAF's leading role in asymmetric response even in traditional operations.

A more sophisticated view recognizes that the USAF ability to deploy and fly its space-based assets anywhere, anytime is essential for contemporary reconnaissance, communication, and command and control. This capability will be even more important in 2025. Discussions of direct broadcast satellite sensor-to-shooter or satellite-to-Joint Surveillance, Targeting, and Reconnaissance System (JSTARS) and then to all relevant parties is a central component of global reach. The capabilities of aircraft like *Commando Solo* or follow-on variants based on UAVs or direct broadcast satellites and the variety of on board electronic warfare wizardry already deployed on most US combat aircraft are recognized, again, as central to global reach. Future requirements for air refueling will include servicing UAVs and UCAVs used for information attack, perhaps via batteries recharged by airborne or satellite-reflected, ground-based lasers.[13]

Many of the current and projected global reach capabilities in speed, lift, and all-weather performance based on ever more precise navigation will be even more central to information warfare and information attack in 2025. As the new generation of sensors based on a distributed system of satellites, surface sensors, and standoff systems is developed, USAF "atmospheric" global-reach thinking must evolve to include the mission of precise, point-of-use delivery of surface-based sensors. Global reach must develop the capability to deliver sensors, or other information attack hardware, with the same stealth, speed and, most importantly,

precision now focused primarily on bombs. Global reach requires that ultra-high altitude air drops of information attack devices via, perhaps, Global Positioning System (GPS) based steerable parachutes must receive the same attention currently given precision guided munitions.[14]

The future role of USAF space reach is, of course, central to global awareness and global power. Specific space-based information warfare capabilities such as direct broadcast of video-morphed news broadcasts by the enemy leader announcing surrender are easy to imagine. These "Hollywood" capabilities, however, may not be the best use of space by the USAF. Whether protecting free access to space, defending against hostile use of commercial satellites by an adversary, developing an antisatellite capability, or having launch-on-demand capabilities, any and all of these could have some application to information attack (and defense). However, as the liberal, free-market, information-based economies of the United States and our allies are among those most likely to depend on "freedom of the high frontier," the USAF should be hesitant about the militarization of space. On the other hand, if information attack is correctly identified as directly corrupting information without visibly changing the physical entity within which it resides, the potential for information attack against the United States or its allies via space-based commercial or neutral third-party systems cannot be ignored.[15] As shutting down the space-based planetary navigation or communications systems may not be an option for either technical or political reasons,[16] USAF global reach to support global awareness and power will require a residual capability to provide launch-on-demand or activation-on-demand of secure systems.

Global Power

USAF global power, increasingly characterized by the ability to engage with precise and discriminating effect, permits the asymmetric strategic response which leverages the differential information-in-war advantage provided by global awareness and the information-based planning and execution control provided by global reach. USAF global air and space power capabilities increasing demonstrate that the USAF's concept of *decisive* maneuver, engagement with precise and differential or relative superiority, should replace the *Joint Vision 2010* concept of *dominant* maneuver.

Dominant maneuver, recall, proposes to bring together widely dispersed joint forces to replace the sequential march through the enemy's fielded military, population, infrastructure, and system essentials to get to the adversary leadership to convince him to change his behavior by attacking the adversary throughout the height, breadth, and depth of the battlespace and by attacking all levels of the enemy's centers of gravity simultaneously. The adversary system goes into shock and its ability to react is paralyzed. Dominant maneuver has become the Holy Grail of joint force employment. In reality, this massive and simultaneous engagement of joint forces appears to be required primarily because the joint force campaign planners lack the real-world, near-real-time knowledge of the key structures and patterns of activity, information, communication, or databases on which the adversary is dependent. *Joint Vision 2010*'s "Full Spectrum Dominance," a very traditional American vision of war fighting, reflects the continuing inability to recognize the potential of information warfare. The emerging mission of USAF global awareness, as noted previously, must be to address this requirement to identify the strategic and militarily-relevant information differential. Dominant maneuver may be an obsolete concept for the exercise of military power in many of the security challenges of the near-future. Decisive maneuver, seen by the USAF as engagement with precise and differential or relatively superior air and space power assets, will be the future strategic choice and the rational use of scarce military resources. It will be the way to do more, differently.

Information warfare in the dominant maneuver universe is likewise usually discussed analogously to cumulative war in that a full-spectrum attack on the adversary's information infrastructure results in rendering him blind, deaf, and dumb. Lacking command and control of his military forces then, his actions are supposed to become chaotic and his forces are thus easier to defeat. It has not, however, been demonstrated that a blinded, chaotic actor represents the enemy decision maker from whom one could expect rational compliance with US strategic objectives.[17] Battle is supposed to be about "some" thing, not "any" thing. Total information warfare against the adversary may be closer to "making the rubble bounce" than intelligent war fighting.

Information attack, on the other hand, as seen by the USAF more narrowly than full-scale IW, will be the essential component of decisive maneuver and may, in some situations, be the only exercise of discriminate power required to shape relatively predictable actions and produce the "strategic situation so advantageous" that US security objectives are met without dominant maneuver of the whole joint team. For

the USAF to develop the capability for discriminate, precision information attack, new USAF research must address precise modeling of a potential adversary's Markov chains [18] and revisit the theories of power distribution control.[19]

Further Refinements

Information warfare can be direct or indirect. While it may appear at first counterintuitive, indirect IW involves creating information (or disinformation) that the adversary must observe if the intended effect is to be achieved.[20] A false radio transmission that is not intercepted by the enemy is a waste of electrons. For the USAF, indirect IW as a form of perception management[21] will be executed in the future most often by the traditional means of command and control warfare: psychological operations, military deception, security measures, electronic warfare, and physical destruction.[22]

Direct information warfare involves changing an adversary's information without involving the requirement that it be observed. Direct information warfare, counterintuitively, bypasses the adversary's perceptive or observing functions.[23] Thus, direct IW will be executed in most cases by information attack: directly corrupting information without visibly changing the physical entity within which it resides.[24] The goal is to "access the adversary's base of information used for decision making, thereby minimizing the unpredictability of the perceptive process."[25] Based on the information provided via USAF global awareness capabilities and the ability to deploy provided by global atmospheric and space reach, both indirect and direct USAF IW capabilities will be developed.

Planning for information attack would need to include the assembly of baseline critical data, the analysis of adversary essential networks or systems, and human activity patterns. Thus, as the essential first step, a vulnerability assessment of the processes, procedures, and physical characteristics of adversary information-dependent activities would need to be developed and continually updated.[26] To prepare to use information attack in asymmetric response, USAF info-warriors in 2025 must be guided by the principle that adversary military force is ultimately an output or peripheral of a weapons system and its sustaining, often

civil, infrastructure.[27] Corrupt the sustaining system and, like a diver deprived of his oxygen supply, the adversary military force may be ineffective.

The chief technical requirements for information attack that would need to be developed by the USAF in 2025 would include awareness of future trapdoors in computer programs and components; future systems to defend and penetrate, in peace and war, critical military, commercial, and educational, information-dependent systems; and future systems to protect against and deploy corrupt information via common carrier globally distributed information systems, false-flag (commercial products), or third-party (coalition partners) systems.[28] Capability for precision stealthy deployment of sensors and information attack devices would need to be developed. Most importantly, alternative sets of databases and communications architectures will need to be developed and kept on the shelf in the future. Returning to the classic North American Air Defense Command model, once the pattern of information-dependent human activities is identified, the information target can be detected and identified, and the data on which the activity is dependent could be intercepted, destroyed, or corrupted by appropriate replacement. Is this science fiction? The Air Force Scientific Advisory Board notes that "methods for attacking information systems are under development"[29]and future "technologies and concepts for intelligence gathering and information attack in the commercially based, distributed global information system of 2025" can be discussed.[30]

If, for example, an emerging peer competitor of the type identified as "Khan" in the *2025 Study* were to conduct missile tests or war games in an area or manner deemed unacceptable to the US or an ally, a standard response might be to redeploy a US carrier battle group to the region to signal or deter. The asymmetric strategic response would be to conduct information warfare through several means. Data could be manufactured and broadcast from USAF satellite assets which showed to all parties listening that Khan's missiles are woefully inaccurate as second-stage burn was only 87 percent complete. This would be indirect IW. The future capability needed for direct IW through information attack would be the insertion of the identical data into Khan's own sensor systems and the sensor systems of third parties, say a regional ally of Khan, to confirm the data. Finally, and most ambitiously, Khan's sensor architecture could be corrupted so that even if true data from, say, a commercial satellite system were examined, the corrupt results would still obtain. That one or two other sources might provide the correct data only complicates further the adversary's

orientation and analytic problems. The battlespace of future conflicts could be shaped by the long-term effects of nonlethal disorientation information attack.

Notes

[1] Robert J. Wood, Information Engineering: The Foundation of Information Warfare, (Maxwell AFB, Ala.: Air War College Research Report, 1995) {available from Air University Library, Maxwell AFB}

[2] Air Force Scientific Advisory Board, New World Vistas: Air and Space Power for the 21st Century - Summary Volume, (1995), 19.

[3] USAF, Air Force Doctrine Document-1, 10.

[4] Air Force Scientific Advisory Board, New World Vistas: Air and Space Power for the 21st Century - Summary Volume (1995), 22–4.

[5] Chips, 14 no.1 (January 1996) special issue on the Defense Message System (DMS).

[6] Martin C. Libicki and Jim Hazlett, "Do We Need and Information Corps?," *Joint Force Quarterly* no. 2 (Autumn 1993), 88–97.

[7] John A. Warden, *The Air Campaign: Planning for Combat* (Washington, D.C.: National Defense University Press, 1988).

[8] Bruce M. DeBlois, *et al*. Dropping the Electric Grid: An Option for the Military Planner (Maxwell AFB, Ala.: Air University Press, 1994).

[9] Air Force Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century - Summary Volume* (1995), 26.

[10] Michael J. Witt, "U.K. To Test Civil Computers in Secure Defense Arena," *Defense News* (1–7 April 1996), 12.

[11] Pat Cooper, "War Game Reveals IW Vulnerabilities," *Defense News* (4–10 March 1996), 33.

[12] *Legal Aspects of Information Warfare Symposium - Conference Proceedings* (Maxwell AFB, Ala.: Air Force Judge Advocate General School, November 1995).

[13] Frank Oliveri, "Unmanned Aircraft May Dominate Air Warfare," *Defense News*, (4–10March 1996), 8.

[14] Air Force Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century - Summary Volume* (1995), 32.

[15] Michael R. Mantz, *The New Sword: A Theory of Space Combat Power*, (Maxwell AFB, Aal.: Air University Press, 1995).

[16] Jennifer Heronema, "Pentagon Must Give Equal Time to Commercial Users of GPS," *Defense News*, (1–7April 1996), 58.

[17] George J. Stein, "Information War - Netwar - Cyberwar," in B. R. Schneider and L. E. Grinter eds., Battlefield of the Future: 21st Century Warfare Issues, (Maxwell AFB, Ala.: Air University Press, 1995), 153–170.

[18] Robert J. Wood, Information Engineering: The Foundation of Information Warfare, (Maxwell AFB, Ala.: Air War College Research Report, 1995), 35-47.

[19] George E. Orr, Combat Operations C3I: Fundamentals and Interactions, (Maxwell AFB, Ala.: Air University Press, 1983).

[20] USAF, *Cornerstones of Information Warfare*, 4.

[21] USAF, Air Force Doctrine Document-5, 7.

[22] Norman B. Hutcherson, Command and Control Warfare: Putting another Tool in the War-fighter's Data Base, (Maxwell AFB, Ala.: Air University Press, 1994).

[23] USAF, Air Force Doctrine Document-5, 7.

[24] Lawrence G. Downs, Digital Data Warfare: Using Malicious Computer Code as a Weapon, (Maxwell AFB, Ala.: Air War College student research project (1995), {available from Air University Library, Maxwell AFB}

[25] USAF, Air Force Doctrine Document-5, 7.

[26] Pat Cooper, "U.S. Must Boost C4I Models, Simulation," *Defense News* (1-7 April 1996), 46.

[27] Frank M. Snyder, *Command and Control: The Literature and Commentaries*, (Washington, D.C.: National Defense University Press, 1993).

[28] Paul DiJulio, *et al.*, "Communications-Computer Systems: Critical Centers of Gravity," in Air Command and Staff College, Air Campaign Course 1993 - Research Projects, (Maxwell AFB, Ala.: ACSC, 1994), 283–294.

[29] Air Force Scientific Advisory Board, New World Vistas: Air and Space Power for the 21st Century - Summary Volume (1995), 42.

[30] Ibid., B–15.

Chapter 5

Into The Future - Information Attack in 2025

Information attack, while "platform-based" in the physical universe of matter and energy, is not the only counterplatform, and the USAF must move its authoritative doctrinal thinking in *AFDD-1* away from the idea that information attack involves only the use of computers and communications.[1]

Indirect information warfare attacks the "observation" level of knowledge at which the information must be perceived to be acted on. In many cases, indirect IW will be platform-to-platform as, for example, offensive and defensive electronic warfare, jamming or other interference systems, and psychological operations via the successor systems to *Commando Solo*. It may, however, rely on nonelectronic old fashioned military deception and psychological operations. Offensive and defensive indirect IW will grow in importance as information dependence creates information targets for an adversary to exploit against the United States. The armed forces could become "vulnerable sophisticates" in the worlds of 2025.[2] Counterplatform is not everything, but counterplatform attack will not be obsolete.

Direct IW as information attack, on the other hand, corrupts the "orientation" level of knowledge so that adversary analysis, whether artificial-intelligence, information-technology based or, most importantly, based in the mind of the human decision maker, decides and acts with full confidence in either the information observed or the integrity of his (machine or human) analytic processes.[3] Information attack, then, may or may not be counterplatform.

The future potential in information warfare to substitute precise and discriminate credible information— whether by the methods of C^2W (deception, PSYOP, or other means) or information attack— to a precise and discriminate target decision maker is the essence of decisive maneuver as it may position the

adversary in space and time, by his own decision, in that strategic situation so disadvantageous "that if it does not of itself produce the decision, its continuation by a battle is sure to achieve this." It is not so much perception management as orientation management. Information is both the target and the weapon: the weapon effect is predictable error. If, on the other hand, information attack fails and battle is necessary to convince the adversary the old-fashioned way, the differential information-in-war advantage provided by global awareness and the information-based planning and execution control provided by global reach may permit decisive maneuver by USAF air and space assets of such speed, precision, and discriminate force that the joint task force never leaves the Continental United States execute its dominant maneuver.

In the future operating environments marked by ambiguity, speed, and precision effect, it will be the relative or differential advantage in information, information processing, and communication and information security that will provide the narrow margin for victory. Future USAF mastery of information attack, through air and space power unconstrained by artificial notions of battlefield-only command and control warfare, could provide those capabilities for asymmetric strategic response based on decisive and differential information advantage in most future security environments.

Information warfare, in this essay, was defined as "actions taken to achieve relatively greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure in order to deny, exploit, influence, corrupt, or destroy those adversary information-based activities thorough command and control warfare and information attack." The only question is whether the USAF is prepared to take those actions.

Notes

[1] USAF, Air Force Doctrine Document-5, 7.

[2] Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," Airpower Journal 9 no. 1 Spring, 1995, 56–65.

[3] Wieslaw Gornicki, "W cieniu bomby L," Przeglad Spoleczny "DZIS," no.11-62 (1 November 1995), 48–60 [translated by the Federal Broadcast Information Service as "In the Shadow of the L-Bomb."] Gornicki calls IW "the absolute ultimate weapon of the White Man" and fears the CIA is slipping viruses into computer software exported to a future "enemy of freedom."